

Patent Record View - JP2008009600A

[Record View Help](#) | [Close Record Viewer](#)[Add to Work File](#) | [Mark Record](#) | [Watch Record](#) | [Document Delivery](#) | [Translate](#) | [Citation Map](#) | [Highlight](#) | [Print](#)**Jump****To:** [Bibliography](#) | [Abstract](#) | [Classes/Indexing](#) | [Legal Status](#) | [Family](#) | [Description](#) | [Citations](#) | [Other](#)[Hide Images Panel](#)[Show Highlighting Panel](#)

JP2008009600A A biometrics system, a processing apparatus, the biometrics method, and a biometrics program

Bibliography

DWPI Title

Biometrics system for, e.g. room entering-and-exiting management system, outputs notification signal to security server, if biometric information of individual corresponds to biometric information concerning emergency condition

Original Title

BIOMETRIC AUTHENTICATION SYSTEM, PROCESSING DEVICE, BIOMETRIC AUTHENTICATION METHOD AND BIOMETRIC AUTHENTICATION PROGRAM

Assignee/Applicant

Standardized: **HITACHI LTD**

Original: HITACHI LTD

Inventor

TOKUNAGA MOTOKATSU; NAKAMURA KENJI

Publication Date (Kind Code)

2008-01-17 (A)

Application Number / Date

JP2006177944A / 2006-06-28

Priority Number / Date / Country

JP2006177944A / 2006-06-28 / JP

Abstract

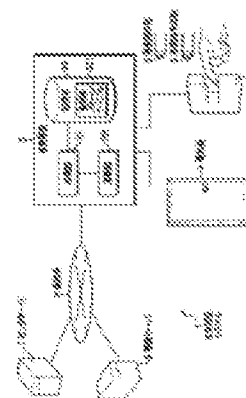
-

Classes/Indexing

IPC

Current IPC Class	Invention	Version	Additional	Version

Images(9)

View in: [Single Row](#)[Scroll to view all images & click to enlarge](#)

(19) 日本国特許庁 (JP)

(12) 公開特許公報(A)

(11) 特許出願公開番号

特開2008-9600

(P2008-9600A)

(43) 公開日 平成20年1月17日 (2008.1.17)

(51) Int. Cl.	F I	テーマコード (参考)
G08B 25/04 (2006.01)	G08B 25/04 G	5B285
G06F 21/20 (2006.01)	G06F 15/00 330F	5C087
G08B 25/10 (2006.01)	G08B 25/10 D	5J104
G08B 25/08 (2006.01)	G08B 25/08 A	
H04L 9/32 (2006.01)	H04L 9/00 673D	
審査請求 未請求 請求項の数 12 O L (全 13 頁)		

(21) 出願番号 特願2006-177944 (P2006-177944)

(22) 出願日 平成18年6月28日 (2006.6.28)

(71) 出願人 000005108

株式会社日立製作所

東京都千代田区丸の内一丁目6番6号

(74) 代理人 100064414

弁理士 磯野 道造

(74) 代理人 100111545

弁理士 多田 悦夫

(72) 発明者 ▲徳▼永 素克

茨城県ひたちなか市市毛1070番地

株式会社日立製作所

都市開発システムグループ内

(72) 発明者 中村 健二

茨城県ひたちなか市市毛1070番地

株式会社日立製作所

都市開発システムグループ内

最終頁に続く

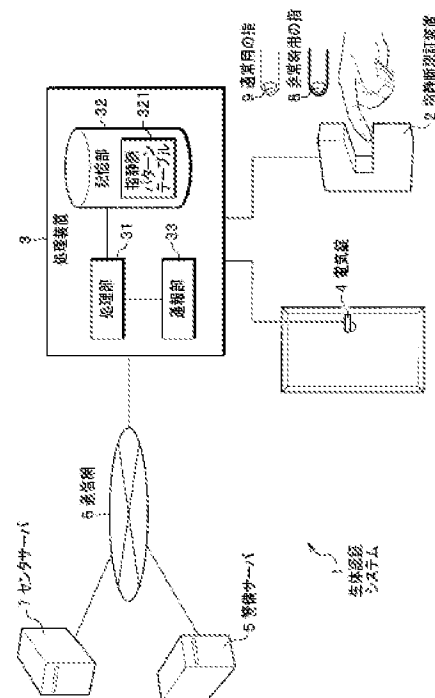
(54) 【発明の名称】 生体認証システム、処理装置、生体認証方法および生体認証プログラム

(57) 【要約】

【課題】 第三者に行動を気づかせることなく、緊急報知を発報することが可能な生体認証システム、処理装置、生体認証方法および生体認証プログラムを提供する。

【解決手段】 電気錠4の開閉錠を制御するための生体認証システム1において、生体情報取得装置2が取得した生体情報が、非常時用の生体情報であるか、通常用の生体情報であるか、を処理装置3が判別し、前記取得した生体情報が、前記非常時用の生体情報である場合は、処理装置3が、警備サーバ5への出力を行い、前記取得した生体情報が、前記通常用の生体情報である場合は、処理装置3が、電気錠4の開錠を行うことを特徴とする。

【選択図】 図1



【特許請求の範囲】**【請求項 1】**

生体認証を行うための生体情報を取得する生体情報取得装置と、前記生体情報取得装置が取得した生体情報を基に、生体認証処理を行う処理装置と、を含んで備える生体認証システムであって、

前記処理装置は、

同一人物から取得した生体情報である第 1 の生体情報と、第 2 の生体情報とを格納する記憶部と、

前記生体情報取得装置から送られた生体情報と、前記記憶部に格納されている前記第 1 の生体情報および前記第 2 の生体情報とを照合することによって、前記送られた生体情報が、前記第 1 の生体情報と一致するか、前記第 2 の生体情報と一致するか、を判別し、

前記判別の結果、前記送られた生体情報が、前記第 1 の生体情報と一致する場合は、第 1 の出力を行う機能を有する処理部と、を含んで備えることを特徴とする生体認証システム。

【請求項 2】

前記処理装置は、前記処理装置に接続された警備サーバに緊急報知を行う機能を有する通報部をさらに備え、

前記第 1 の出力とは、前記通報部に、前記警備サーバへの緊急報知を行わせる信号の出力ことであることを特徴とする請求項 1 に記載の生体認証システム。

【請求項 3】

前記処理部は、

前記判別の結果、

前記送られた生体情報が、前記第 2 の生体情報と一致する場合は、第 2 の出力を行う機能をさらに有することを特徴とする請求項 1 または請求項 2 に記載の生体認証システム。

【請求項 4】

前記生体認証システムは、前記処理装置により錠の開閉が可能な電気錠をさらに備え、

前記第 2 の出力とは、前記電気錠を開錠させる信号の出力であることを特徴とする請求項 3 に記載の生体認証システム。

【請求項 5】

前記生体認証システムは、前記処理装置に接続されたコンピュータをさらに備え、

前記第 2 の出力とは、前記コンピュータへログインする信号の出力であることを特徴とする請求項 3 に記載の生体認証システム。

【請求項 6】

前記生体認証システムは、前記処理装置に接続された現金取引装置をさらに備え、

前記第 2 の出力とは、前記現金取引装置に、現金の取引処理を行わせる信号の出力であることを特徴とする請求項 3 に記載の生体認証システム。

【請求項 7】

前記処理装置は、

前記第 1 の出力を行った後、前記第 2 の生体情報と一致する生体情報が、前記生体情報取得装置から送られてきた場合、前記第 1 の出力が誤りである旨の信号を出力する機能をさらに有することを特徴とする請求項 1 から請求項 6 のいずれか一項に記載の生体認証システム。

【請求項 8】

前記生体情報とは、静脈パターン、指紋パターン、虹彩パターン、または網膜の血管パターンであることを特徴とする請求項 1 から請求項 7 のいずれか一項に記載の生体認証システム。

【請求項 9】

生体認証を行うための生体情報を取得する生体情報取得装置と、前記生体情報取得装置が取得した生体情報を基に、生体認証処理を行う処理装置と、を含んで備える生体認証システムにおける処理装置であって、

10

20

30

40

50

同一人物から取得した生体情報である第 1 の生体情報と、第 2 の生体情報とを格納する記憶部と、

前記生体情報取得装置から送られた生体情報と、前記記憶部に格納されている前記第 1 の生体情報および前記第 2 の生体情報とを照合することによって、前記送られた生体情報が、前記第 1 の生体情報と一致するか、前記第 2 の生体情報と一致するか、を判別し、

前記判別の結果、前記送られた生体情報が、前記第 1 の生体情報と一致する場合は、第 1 の出力を行う機能を有する処理部と、を含んで備えることを特徴とする処理装置。

【請求項 10】

生体認証を行うための生体情報を取得する生体情報取得装置と、前記生体情報取得装置が取得した生体情報を基に、生体認証処理を行う処理装置と、を含んで備える生体認証システムの生体認証方法であって、

前記処理装置は、

同一人物から取得した生体情報である第 1 の生体情報と、第 2 の生体情報とを格納する記憶部と、情報を処理する処理部と、を有してなり、

前記処理部が、

前記生体情報取得装置から送られた生体情報と、前記記憶部に格納されている前記第 1 の生体情報および前記第 2 の生体情報とを照合することによって、前記送られた生体情報が、前記第 1 の生体情報と一致するか、前記第 2 の生体情報と一致するか、を判別し、

前記判別の結果、前記送られた生体情報が、前記第 1 の生体情報と一致する場合は、第 1 の出力を行うことを特徴とする生体認証方法。

【請求項 11】

生体認証を行うための生体情報を取得する生体情報取得装置と、前記生体情報取得装置が取得した生体情報を基に、生体認証処理を行う処理装置と、を含んで備える生体認証システムにおける処理装置の生体認証方法であって、

前記処理装置は、

同一人物から取得した生体情報である第 1 の生体情報と、第 2 の生体情報とを格納する記憶部と、情報を処理する処理部と、を有してなり、

前記処理部が、

前記生体情報取得装置から送られた生体情報と、前記記憶部に格納されている前記第 1 の生体情報および前記第 2 の生体情報とを照合することによって、前記送られた生体情報が、前記第 1 の生体情報と一致するか、前記第 2 の生体情報と一致するか、を判別し、

前記判別の結果、前記送られた生体情報が、前記第 1 の生体情報と一致する場合は、第 1 の出力を行うことを特徴とする生体認証方法。

【請求項 12】

請求項 10 または請求項 11 の生体認証方法を、コンピュータに実行させることを特徴とする生体認証プログラム。

【発明の詳細な説明】

【技術分野】

【0001】

本発明は、入退室管理システムや情報セキュリティシステムなどの個人認証に生体情報を使用する技術に関する。

【背景技術】

【0002】

従来、通常利用するカード以外にもう 1 枚のカードを非常時用に用意しておき、カードの情報が入力された場合に、この入力されたカードの情報が通常利用されるカード（通常用カード）の情報か、非常時用のカード（非常用カード）の情報かを認識し、非常用カードの情報であれば、警備会社などへ通報する現金取引システムおよび現金取引装置が提示されている（例えば、特許文献 1 参照）。

また、通報者が、携帯する記憶手段の個人情報情報を非接触で読み出し、認証情報メモリに格納されている認証情報と、前記した個人情報とを照合し、認証を行った後、緊急通報と

10

20

30

40

50

ともに、個人情報も通知する緊急通報システムが提示されている（例えば、特許文献2参照）。

【0003】

さらに、個人を認証し、その認証結果に連動したドア制御や、P C（Personal Computer）へのログイン機能などをもつ入退室管理システムや情報セキュリティシステム（総称して認証システムと記載する）などにおいて、認証精度や、セキュリティ性を向上すべく、生体情報を用いて、生体認証を行う認証システム（生体認証システム）がある。このような生体認証システムでは、認証登録された個人（登録者）以外の人が悪意的に入室や、P Cへのログインをしようとしても、登録された生体情報を偽造することは難しいので、登録者自身の身体を使用しない限りは容易に入室、またはP Cへのログインが出来ない、セキュリティ性の高いシステムを構築することができる。

10

【特許文献1】特開2000-182122号公報（請求項1）

【特許文献2】特開2003-309666号公報（段落0015～0016）

【発明の開示】

【発明が解決しようとする課題】

【0004】

ところで、特許文献1に記載されている技術では、登録者は、通常用カード及び非常用カードを常に携帯していなければならない、管理負担が増大する。また、カードの管理センタなどの管理側でも、管理する情報量が増え、やはり管理負担が増大し、ランニングコストが高くなるといった問題がある。

20

【0005】

また、前記したような生体認証システムにおいて、侵入者が入室、またはP Cへのログインを行なおうとする場合、登録者を脅し、入室、またはP Cへのログインを無理矢理させようとするケースが発生する。その際、従来システムにおいては、侵入異常の緊急報知を発生させるため、テンキーによる緊急用の暗証番号の入力や非常ボタンを押すことで緊急報知を発報させる必要がある。しかし、この緊急報知発生方法は通常の認証動作とは違う動作を行うため、侵入者に緊急報知発生動作をしていることが分かってしまう可能性があり、身の安全面などでの危険性がある。

特許文献2における緊急通報システムにおいても、緊急時の場合には、非常押しボタンを押下する動作を行うため、同様の危険性がある。

30

【0006】

このような背景に鑑みて本発明がなされたのであり、本発明は、第三者に行動を気づかせることなく、緊急報知を発報することが可能な生体認証システム、処理装置、生体認証方法および生体認証プログラムを提供することを目的とする。

【課題を解決するための手段】

【0007】

前記課題を解決するため、本発明を完成するに至った。すなわち、本発明の生体認証システム、処理装置、生体認証方法および生体認証プログラムは、生体情報取得装置が取得した生体情報が、第1の生体情報であるか、第2の生体情報であるか、を処理装置が判別し、前記取得した生体情報が、前記第1の生体情報である場合は、処理装置が、第1の出力を行うことを特徴とする。

40

【発明の効果】

【0008】

本発明によれば、第三者に行動を気づかせることなく、緊急報知を発報することが可能となる。

【発明を実施するための最良の形態】

【0009】

次に、本発明を実施するための最良の形態（「実施形態」という）について、適宜図面を参照しながら詳細に説明する。

本実施形態では、生体認証システム1を、入退室管理システムに適用した例について説

50

明する。

【0010】

(第1実施形態：システム構成)

【0011】

図1は、第1実施形態にかかる生体認証システムの構成図である。

生体認証システム1は、以下の各装置を備えてなる。

指静脈認証装置2（請求項における生体情報取得装置）は、ユーザの指から静脈のパターンデータ（指静脈パターン）を抽出し、抽出した指静脈パターンを処理装置3に送信する。

処理装置3は、指静脈認証装置2と接続しており、指静脈認証装置2から送信された指静脈パターンが、処理装置3に、予め登録してある非常時用の指8の静脈パターン（非常用指静脈パターン：請求項における第1の生体情報）と一致するか、通常用の指9の静脈パターン（通常用指静脈パターン：請求項における第2の生体情報）と一致するか、を判定し、それぞれの指静脈パターンに応じた処理を行う。

電気錠4は、処理装置3と接続しており、処理装置3から開錠の指示があると、自身を開錠する。

【0012】

警備サーバ5は、警備センタなどに設置され、公衆回線網、移動体通信網、インターネットなどからなる通信網6を介して、処理装置3と接続している。警備サーバ5は、通信網6を介して、処理装置3から緊急報知を受信すると、警備員を現場に向かわせる通知を行う。

また、生体認証システム1は、通信網6を介して、処理装置3と接続され、処理装置3に格納されている通常用指静脈パターンや、非常用指静脈パターンをバックアップしたり、緊急報知履歴を保存したりするセンタサーバ7を備えてもよい。

【0013】

なお、指静脈認証装置2は、<http://www.hitachi.co.jp/Product/comp/fingervein/pdf/05joumyaku0510.pdf>に概要が記載されている。また、指静脈認証装置2と電気錠4とを用いた入退室管理システムは、<http://www.hitachi-hec.co.jp/newsrel/20030901.htm>に概要が記載されている。

【0014】

処理装置3は、情報を処理する処理部31と、通常用指静脈パターン、および非常用指静脈パターンを含む指静脈パターンテーブル321を格納する記憶部32と、警備サーバ5へ、緊急報知する通報部33とを備える。

ここで、通常用指静脈パターン、および非常用指静脈パターンは、それぞれ同一人物から取得された指静脈パターンである。

通常用指静脈パターン、および非常用指静脈パターンの例として、例えば、右手の人差指の静脈パターンを通常用指静脈パターンとし、左手の人差指の静脈パターンを非常用指静脈パターンとするケースや、人差指の静脈パターンを通常用指静脈パターンとし、中指の静脈パターンを非常用指静脈パターンとするケースなどが考えられる。

また、本実施形態では、記憶部32は、処理装置3と一体になっているとしたが、これに限らず別個の装置としてもよい。

【0015】

なお、図1に示す処理装置3の、処理部31および通報部33は、記憶部32に記憶されているプログラムが、図示しないRAM（Random Access Memory）に展開され、図示しないCPU（Central Processing Unit）により、実行されることによって具現化する。

【0016】

図2は、記憶部に格納される指静脈パターンテーブルの例を示す図である。

指静脈パターンテーブル321は、ユーザ名（ユーザA、ユーザB、・・・）に対応する形で、通常用指静脈パターン（通常用指静脈パターンA1、通常用指静脈パターンB1

10

20

30

40

50

、・・・)および非常用指静脈パターン(非常用指静脈パターンA2、非常用指静脈パターンB2、・・・)が格納される。

指静脈パターンテーブル321は、処理装置3の図示しない入力部を介して、情報を入力することによって、管理者によって、図3に示す処理に先立って作成される。

なお、ユーザ名の代わりに、ユーザID(Identification)やカードIDとしてもよい。

【0017】

(システム処理)

次に、図1を参照しつつ、図3に沿って本実施形態に係る生体認証方法を説明する。

図3は、第1実施形態に係る生体認証方法の処理の流れを示すフローチャートである。

まず、処理装置3、指静脈認証装置2および電気錠4の電源がONにされると、処理装置3および指静脈認証装置2は、入力待ち状態となる(S1)。

そして、登録者が、指を指静脈認証装置2に挿入すると、指静脈認証装置2は、挿入された指の静脈パターンをパターンデータ(指静脈パターン)として取得する(S2)。このとき、緊急時であれば、登録者は、非常用指静脈パターンとして登録しておいた指(図1における非常時用の指8)を、指静脈認証装置2に挿入し、緊急時でなければ(すなわち、通常時)、登録者は、通常用指静脈パターンとして登録しておいた指(図1における通常用の指9)を、指静脈認証装置2に挿入する。

次に、指静脈認証装置2は、抽出した指静脈パターンを、処理装置3に送信する(S3)。

【0018】

そして、処理装置3の処理部31は、送信された指静脈パターンを、記憶部32に格納されている指静脈パターンと照合して、登録されている指静脈パターンと一致するか否かを判定する(S4)。

ステップS4の判定の結果、登録されている指静脈パターンと一致しない場合(S4→No)、生体認証システム1は、ステップS1へ処理を戻す。また、ここで処理部31が、指静脈認証装置2の図示しない表示部にエラーメッセージを表示させたり、通報部33に警備サーバ5へ緊急報知させたりしてもよい。

ステップS4の判定の結果、登録されている指静脈パターンと一致した場合(S4→Yes)、生体認証システム1は、ステップS5に処理を進める。

【0019】

次に、ステップS3で、指静脈認証装置2から送信された指静脈パターンが、通常用指静脈パターンと一致するか否か、非常用指静脈パターンと一致するか否かを、処理部31が、記憶部32を照合することによって判定する(S5)。

ステップS5の判定の結果、通常用指静脈パターンと一致する場合(S5→通常用)、処理部31は、電気錠4に、開錠するよう指示する(請求項における第2の出力)。そして、指示を受けた電気錠4は、電気錠4自身を開錠し(S6)、生体認証システム1は、ステップS1へ処理を戻す。

ステップS5の判定の結果、非常用指静脈パターンと一致する場合(S5→非常用)、通報部33に、警備サーバ5へ緊急報知するよう指示する(請求項における第1の出力)。指示を受けた通報部33は、通信網6を介して、警備サーバ5へ緊急報知し(S7)、生体認証システム1は、ステップS1に処理を戻す。なお、ここで、警備サーバ5へ緊急報知するのではなく、指静脈認証装置2に備えられている図示しない警報出力部によって、例えばサイレンなどの警報を発してもよい。また、ステップS7の処理時に、通報部33による警備サーバ5への緊急報知の日時や、緊急報知した処理装置3のIP(Internet Protocol)アドレスなどを、処理部31が、通信網6を介してセンタサーバ7に送信し、センタサーバ7は、送信された日時やIPアドレスを緊急報知履歴として、保存してもよい。

【0020】

(第2実施形態：誤報通知)

10

20

30

40

50

次に、図 1 を参照しつつ、図 4 に沿って、緊急時ではないのに、誤って非常用の指 8 を指静脈認証装置 2 に挿入してしまった場合、出力されてしまった緊急報知が誤報である旨を警備サーバ 5 に通知する処理を説明する。

なお、図 4 において、ステップ S 1 からステップ S 7 までは、図 3 と同様の処理であるため、同一の符号を付して説明を省略する。

また、第 2 実施形態にかかる生体認証システム 1 および指静脈パターンテーブル 3 2 1 は、図 1 および図 2 において説明されているものと同様のため、説明を省略する。

【0021】

図 4 は、第 2 実施形態に係る生体認証方法の処理の流れを示すフローチャートである。

ステップ S 7 の処理の後、処理部 3 1 は、予め設定してある所定時間（例えば 1 分間）内に、指静脈認証装置 2 から通常用指静脈パターンと一致する指静脈パターンが送信されたか否か、すなわち通常用の指 9 の静脈パターンが送信されたか否かを判定する（S 8）。具体的には、処理部 3 1 は、ステップ S 7 の後、入力待ち状態となる。そして、指静脈認証装置 2 から、指静脈パターンが送信されると、処理部 3 1 は、ステップ S 4 およびステップ S 5 と同様の処理を行うことによって、ステップ S 8 の判定を行う。

ステップ S 8 の判定の結果、所定時間内に通常用の指 9 の静脈パターンが送信された場合（S 8 → Yes）、処理部 3 1 は、ステップ S 7 で通知した緊急報知は、誤りである旨の通知をするよう通報部 3 3 に指示する。指示を受けた通報部 3 3 は、ステップ S 7 で通知した緊急報知が、誤り（誤報）である旨の通知を、警備サーバ 5 に対して行う（S 9）。当該通知を受信した警備サーバ 5 は、警備員に対してステップ S 7 で受信した緊急報知は、誤り（誤報）である旨の通知を行う（S 10）。そして、生体認証システム 1 は、ステップ S 1 に処理を戻す。

【0022】

ステップ S 8 の判定の結果、所定時間内に通常用の指 9 の静脈パターンが送信されなかった場合（S 8 → No）、通報部 3 3 は、そのまま警備サーバ 5 に対して、緊急報知を続ける（S 7）。

警備サーバ 5 に対する緊急報知が終了すると、生体認証システム 1 は、ステップ S 1 に処理を戻す。警備サーバ 5 への緊急報知は、ステップ S 7 の緊急報知開始から、例えば予め設定してある所定時間経過したら、自動的に終了させてもよい。あるいは、緊急報知を受信した警備サーバ 5 が、緊急報知に対する応答を、通信網 6 を介して処理装置 3 に送信し、応答を受信した処理装置 3 が警備サーバ 5 への緊急報知を終了してもよい。また、図示しない処理部 3 1 の入力部を介して、緊急報知の終了コマンドが入力されることによって、警備サーバ 5 への緊急報知を終了してもよい。

【0023】

（第 3 実施形態：指紋）

次に、図 5 から図 7 を参照して、生体情報に指紋を用いた場合について説明する。

なお、図 5 から図 7 において、図 1 から図 3 と同様の要素または処理については、同一の符号をふって説明を省略する。

【0024】

図 5 は、第 3 実施形態にかかる生体認証システムの構成図である。

生体認証システム 1 a は、以下の各装置を備えてなる。

指紋認証装置 2 a（請求項における生体情報取得装置）は、ユーザの指から指紋のパターンデータ（指紋パターン）を抽出し、抽出した指紋パターンを処理装置 3 a に送信する。

処理装置 3 a は、指紋認証装置 2 a と接続しており、指紋認証装置 2 a から送信された指紋パターンが、処理装置 3 a に、予め登録してある非常時用の指 8 の指紋パターン（非常用指紋パターン：請求項における第 1 の生体情報）と一致するか、通常用の指 9 の指紋パターン（通常用指紋パターン：請求項における第 2 の生体情報）と一致するか、を判定し、それぞれの指紋パターンに応じた処理を行う。

【0025】

処理装置 3 a が、第 1 実施形態および第 2 実施形態の処理装置 3（図 1 参照）と異なる点は、通常用指紋パターン、および非常用指紋パターンを含む指紋パターンテーブル 3 2 2 を格納する記憶部 3 2 a を備える点である。

ここで、通常用指紋パターン、および非常用指紋パターンは、それぞれ同一人物から取得された指紋パターンである。

通常用指紋パターン、および非常用指紋パターンの例として、例えば、右手の人差指の指紋パターンを通常用指紋パターンとし、左手の人差指の指紋パターンを非常用指紋パターンとするケースや、人差指の指紋パターンを通常用指紋パターンとし、中指の指紋パターンを非常用指紋パターンとするケースなどが考えられる。

また、本実施形態では、記憶部 3 2 a は、処理装置 3 a と一体になっているとしたが、これに限らず別個の装置としてもよい。

【0026】

なお、図 5 に示す処理装置 3 a の、処理部 3 1 および通報部 3 3 は、記憶部 3 2 a に記憶されているプログラムが、図示しない R A M（Random Access Memory）に展開され、図示しない C P U（Central Processing Unit）により、実行されることによって具現化する。

【0027】

図 6 は、記憶部に格納される指紋パターンテーブルの例を示す図である。

指紋パターンテーブル 3 2 2 は、ユーザ名（ユーザ A、ユーザ B、・・・）に対応する形で、通常用指紋パターン（通常用指紋パターン A 3、通常用指紋パターン B 3、・・・）および非常用指紋パターン（非常用指紋パターン A 4、非常用指紋パターン B 4、・・・）が格納される。

指紋パターンテーブル 3 2 2 は、処理装置 3 a の図示しない入力部を介して、情報を入力することによって、管理者によって、図 7 に示す処理に先立って作成される。

なお、ユーザ名の代わりに、ユーザ I D（Identification）やカード I D としてもよい。

【0028】

（システム処理）

次に、図 5 を参照しつつ、図 7 に沿って本実施形態に係る生体認証方法を説明する。

図 7 は、第 3 実施形態における生体認証方法の処理の流れを示すフローチャートである。

ステップ S 1 の後、登録者が、指を指紋認証装置 2 a に挿入すると、指紋認証装置 2 a は、挿入された指の指紋パターンをパターンデータ（指紋パターン）として取得する（S 2 1）。このとき、緊急時であれば、登録者は、非常用指紋パターンとして登録しておいた指（図 5 における非常時の指 8）を、指紋認証装置 2 a に挿入し、緊急時でなければ（すなわち、通常時）、登録者は、通常用指紋パターンとして登録しておいた指（図 5 における通常時の指 9）を、指紋認証装置 2 a に挿入する。

次に、指紋認証装置 2 a は、抽出した指紋パターンを、処理装置 3 a に送信する（S 2 2）。

【0029】

そして、処理装置 3 a の処理部 3 1 は、送信された指紋パターンを、記憶部 3 2 a に格納されている指紋パターンと照合して、登録されている指紋パターンと一致するか否かを判定する（S 2 3）。

ステップ S 2 3 の判定の結果、登録されている指紋パターンと一致しない場合（S 2 3 → N o）、生体認証システム 1 a は、ステップ S 1 へ処理を戻す。また、ここで処理部 3 1 が、指紋認証装置 2 a の図示しない表示部にエラーメッセージを表示させたり、通報部 3 3 に警備サーバ 5 へ緊急報知させたりしてもよい。

ステップ S 2 3 の判定の結果、登録されている指紋パターンと一致した場合（S 2 3 → Y e s）、生体認証システム 1 a は、ステップ S 2 4 に処理を進める。

【0030】

10

20

30

40

50

次に、ステップ S 2 2 で、指紋認証装置 2 a から送信された指紋パターンが、通常用指紋パターンと一致するか否か、非常用指紋パターンと一致するか否かを、処理部 3 1 が、記憶部 3 2 a を照合することによって判定する (S 2 4)。

ステップ S 2 4 の判定の結果、通常用指紋パターンと一致する場合 (S 2 4 → 通常用)、処理部 3 1 は、電気錠 4 に、開錠するよう指示する (請求項における第 2 の出力)。そして、指示を受けた電気錠 4 は、電気錠 4 自身を開錠し (S 6)、生体認証システム 1 は、ステップ S 1 へ処理を戻す。

ステップ S 2 4 の判定の結果、非常用指紋パターンと一致する場合 (S 2 4 → 非常用)、通報部 3 3 に、警備サーバ 5 へ緊急報知するよう指示する (請求項における第 1 の出力)。指示を受けた通報部 3 3 は、通信網 6 を介して、警備サーバ 5 へ緊急報知し (S 7)、処理部 3 1 は、ステップ S 1 に処理を戻す。

なお、ここで、警備サーバ 5 へ緊急報知するのではなく、指紋認証装置 2 a に備えられている図示しない警報出力部によって、例えばサイレンなどの警報を発してもよい。また、ステップ S 7 の処理時に、通報部 3 3 による警備サーバ 5 への緊急報知の日時や、緊急報知した処理装置 3 a の IP (Internet Protocol) アドレスなどを、処理部 3 1 が、通信網 6 を介してセンタサーバ 7 に送信し、センタサーバ 7 は、送信された日時や IP アドレスを緊急報知履歴として、保存してもよい。

【0031】

また、第 2 実施形態の処理における指静脈パターンを、指紋パターンとすることも可能である。

この場合、図 4 の説明における指静脈パターンが、指紋パターンとなる。

【0032】

第 1 実施形態から第 3 実施形態では、生体情報として、指静脈パターンおよび指紋パターンを用いたが、これに限らず掌の静脈パターン、虹彩パターン、網膜の血管パターンなどを用いてもよい。この場合、例えば同一人物における左右のパターンの違いなどから、通常用の生体情報と、非常用の生体情報とに分ける。

また、これらの生体情報を用いた場合、図 1 の指静脈認証装置 2 は、それぞれ掌静脈認証装置、虹彩認証装置、網膜認証装置などとなる。さらに、これらの生体情報を用いた場合、処理装置 3 の記憶部 3 2 に格納される指静脈パターンテーブル 3 2 1 は、掌静脈パターンテーブル、虹彩パターンテーブル、網膜パターンテーブルなどになる。そして、図 3

【0033】

また、第 1 実施形態から第 3 実施形態における生体認証システム 1 は、電気錠 4 を用いた入退室管理システムとしたが、これに限らず PC のログインの際の本人確認に用いることも可能である。

この場合、図 1 における電気錠 4 は、PC となる。そして、図 3 および図 4 のステップ S 6 における「電気錠 4 の開錠」は、「PC へのログイン」となる。

また、現金自動預け払い機 (ATM: Automatic Teller Machine) や、現金自動支払機 (CD: Cash Dispenser) などの現金取引装置における現金の取引処理での本人確認に用

いることも可能である。

この場合、図 1 における電気錠 4 は、ATM や CD などとなる。そして、図 3 および図 4 および図 7 のステップ S 6 における「電気錠 4 の開錠」は、「ATM や CD などの現金の取引処理開始」となる。

そして、PC へのログインや、ATM や、CD などを、第 1 実施形態から第 3 実施形態に適用した例においても、指静脈パターンや、指紋パターンの他に、掌の静脈パターン、虹彩パターン、網膜の血管パターンなどを生体情報として用いることは、当然可能である。

【0034】

(効果)

10

20

30

40

50

本実施形態によれば、緊急時において、指静脈認証装置 2 や指紋認証装置 2 a に挿入する指を、例えば左手の人差指から、右手の人差指に交換するだけで、警備センタへ通知することができるため、第三者に気づかれることなく、警備センタへ通知することが可能となる。

また、指静脈パターンや指紋パターンのような生体情報を認証情報として用いることにより、セキュリティ性が向上する上、登録者がカードなどを常時携帯する必要がなくなり、登録者の管理負担が軽減する。

さらに、カードの管理会社などが、カードを管理する必要がなくなるため、ランニングコストを削減することが可能となる。

【図面の簡単な説明】

10

【0035】

【図 1】第 1 実施形態にかかる生体認証システムの構成図である。

【図 2】記憶部に格納される指静脈パターンテーブルの例を示す図である。

【図 3】第 1 実施形態に係る生体認証方法の処理の流れを示すフローチャートである。

【図 4】第 2 実施形態に係る生体認証方法の処理の流れを示すフローチャートである。

【図 5】第 3 実施形態にかかる生体認証システムの構成図である。

【図 6】記憶部に格納される指紋パターンテーブルの例を示す図である。

【図 7】第 3 実施形態における生体認証方法の処理の流れを示すフローチャートである。

【符号の説明】

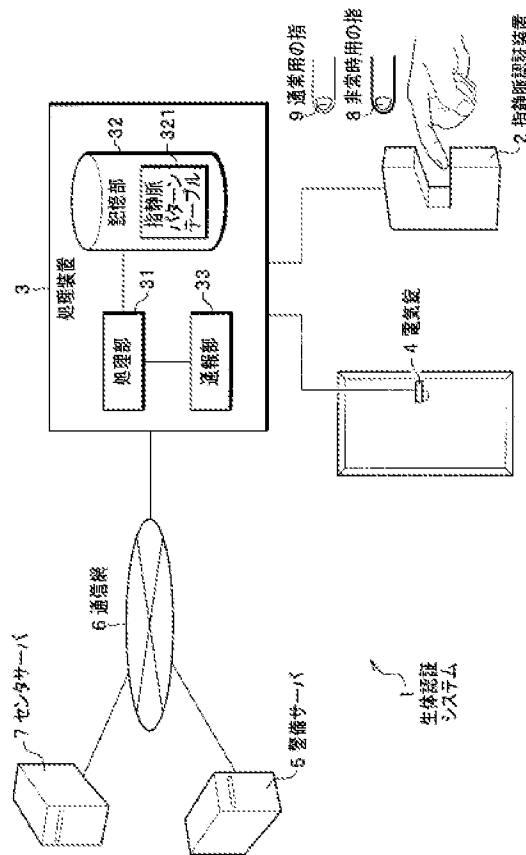
【0036】

20

- 1 生体認証システム
- 2 指静脈認証装置
- 2 a 指紋認証装置
- 3, 3 a 処理装置
- 4 電気錠
- 5 警備サーバ
- 6 通信網
- 7 センタサーバ
- 8 非常時用の指
- 9 通常用の指
- 3 1 処理部
- 3 2, 3 2 a 記憶部
- 3 3 通報部
- 3 2 1 指静脈パターンテーブル
- 3 2 2 指紋パターンテーブル

30

【図 1】

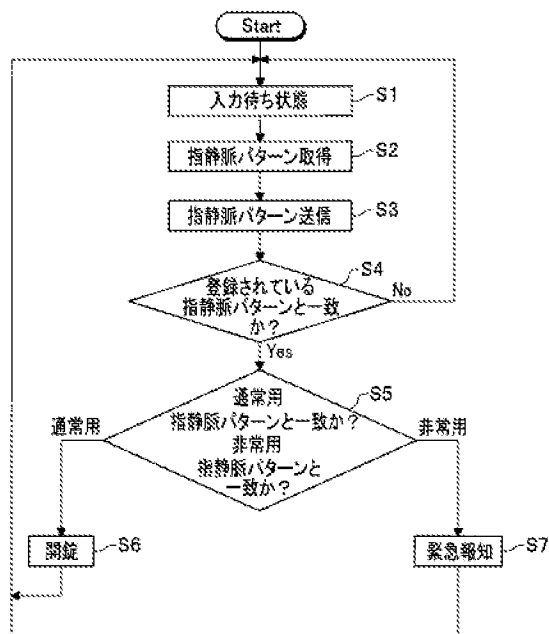


【図 2】

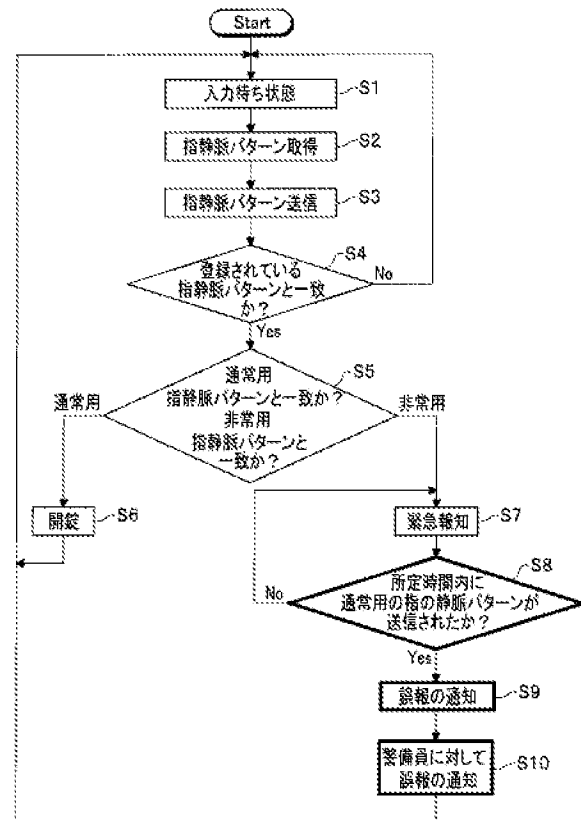
321 指静脈パターンテーブル

ユーザ名	通常用指静脈パターン	非常用指静脈パターン
ユーザA	通常用指静脈パターンA1	非常用指静脈パターンA2
ユーザB	通常用指静脈パターンB1	非常用指静脈パターンB2
⋮	⋮	⋮
⋮	⋮	⋮

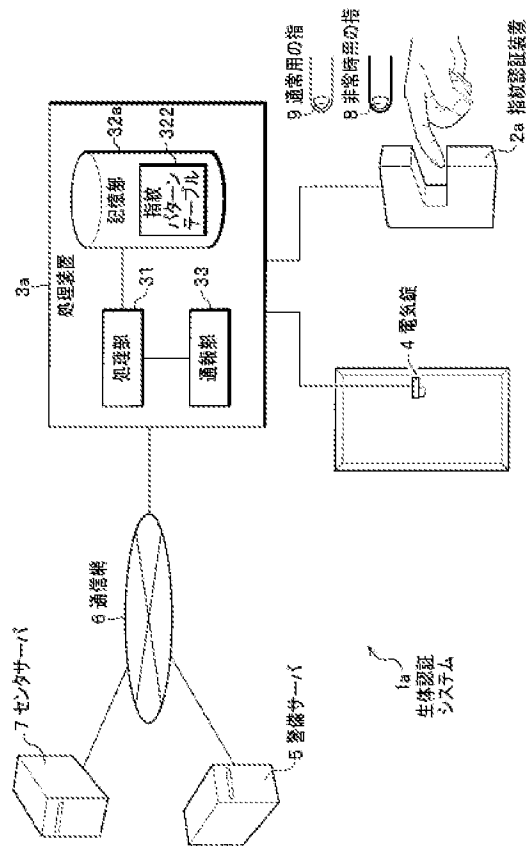
【図 3】



【図 4】



【図 5】

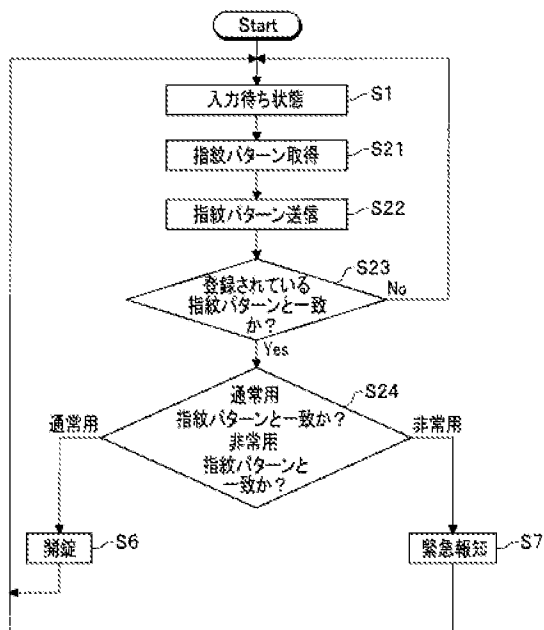


【図 6】

322 指紋パターンテーブル

ユーザ名	通常用指紋パターン	非常用指紋パターン
ユーザA	通常用指紋パターンA3	非常用指紋パターンA4
ユーザB	通常用指紋パターンB3	非常用指紋パターンB4
⋮	⋮	⋮
⋮	⋮	⋮

【図 7】



フロントページの続き

Fターム(参考) 5B285 AA04 CB12 CB15
5C087 AA02 BB11 BB12 BB74 DD03 DD05 DD06 FF01 FF02 GG19
GG20 GG46 GG66
5J104 KA01 KA16 PA16